Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Interface de gestion d'annuaire PHP et sécurisation du réseau.

BARUSELLI Mathieu

I2M Marseille

Responsable entreprise : CHABROL Olivier

Responsable académique : NGUYEN Cong tin

2017

Remerciements

Je tiens tout particulièrement à remercier mes responsables de stage Olivier Chabrol et Pierre Barthélémy pour leur accueil, ainsi que pour la confiance qu'ils m'ont accordée.

Je remercie également Augustino de Souza pour son soutien technique durant le stage.

D'une façon plus générale, je remercie l'ensemble de l' I2M pour l'intérêt qu'ils ont porté à mon travail sur la période de mon stage, ainsi que pour leurs enseignements.

Je remercie de même mon tuteur de stage pour son encadrement pendant celui-ci.

Sommaire

I. Introduction.

1. Historique du laboratoire de Mathématiques.

L'institut de Mathématiques de Marseille (I2M) est une unité mixte de recherche, créée le 1er janvier 2014.

Il a pour tutelles le CNRS, l'université d'Aix-Marseille et l' École Centrale de Marseille.
L'institut est localisé sur trois sites; le technopole de Chateau-Gombert, le campus de Luminy et sur le centre St Charles.

L'I2M est composé de 14 ingénieurs, de 160 chercheurs permanents, dont 26 chercheurs CNRS et 134 enseignants-chercheurs et d'une centaine de chercheurs non-permanents.

Par ailleurs, l'institut compte plus de 40 partenaires publics et privés hors des mathématiques dans de nombreux secteurs comme la physique, la chimie, la santé, ou encore l'industrie.

2. Environnement de travail du pole informatique.

Le service informatique de L'I2M compte 4 personnes, réparties sur l'ensemble des sites.
Sur le pôle de Chateau-Gombert, une cohabitation avec le département informatique de l'université d'Aix-Marseille, la DOSI, est en place.

De ce fait, certains équipements réseaux, et serveurs sont partagés par les deux entités.
La collaboration des deux services est donc nécessaire au bon fonctionnement du laboratoire puisque de nombreuses ressources sont partagées.

Il est également important de noter que le laboratoire dispose d'un plan d'adressage IP particulier, puisque l'ensemble des terminaux disposent d'une adresse publique afin de fournir un débit internet optimal aux utilisateurs, car aucune technologie NAT n'est nécessaire pour accéder à internet.

Le parc informatique de l'institut est composé à 95% d'ordinateur sous Os X (Apple) et à 5% d'ordinateur sous Unix.

I. II.Enoncé des projets réalisés à l'I2M.

1. Descriptif des missions.

L'I2M de Luminy, reçoit quotidiennement de nombreux invités dans ses locaux.
Afin de leurs fournir une connexion internet filaire, il est nécessaire qu' un administrateur renseigne sur un fichier de configuration, les informations nécessaires sur les invités.
Une de mes missions consistait donc à mettre en oeuvre une page web couplée à un script bash pour automatiser cette tâche afin de faciliter l'arrivée et le départ des invités.
Avec la constante évolution de l'informatique, il est nécessaire d'améliorer quotidiennement les services d'une entreprise, pour cela différentes tâches m'ont été affectées sur le site de Château-Gombert:

-Le déploiement d'un serveur de virtualisation pour les services du laboratoire :

Installation d'un environnement de virtualisation Open Sources nommé Proxmox basé sur kvm et Debian afin d'installer différentes applications d'entreprise.

-La redondance du stockage du serveur de virtualisation :

Il s'agit de mettre en place une technologie "RAID" sur les disques d'un serveur afin d'augmenter la tolérance aux pannes.

-La mise en place de service de supervison réseau :

Installation et comparaisons des solutions Open Sources de supervision réseau nommé Shinken et Icinga2, qui ont pour but de faciliter le dépannage du réseau.

-L'installation d'un annuaire informatique :

Mise en place d'un annuaire informatique Open Sources nommé OpenLDAP pour authentifier les utilisateurs sur les ordinateurs.

-L'augmentation de la sécurité des équipements réseaux :

Modification des protocoles de connexions aux équipements réseaux afin de garantir une sécurité supplémentaire.

-La conception d'un interface web de gestion d'annuaires :

Création d'une interface web en PHP afin de modifier, supprimer ou ajouter un utilisateur dans l'annuaire de l'entreprise.

-Optimisation de la topologie réseau :

Remplacement d'équipements réseau obsolètes et suppressions des configurations désuètes.

-La rédaction de documentation technique :

Ajout de documentation dans le Wiki de l'entreprise pour faciliter le dépannage pour les techniciens sur les tâches réalisées durant le stage.

2. Implémentation d'un annuaire informatique LDAP.

a. Qu'est-ce qu'un annuaire informatique ?

Dans une entreprise, les applications ont besoin de droits d'accès pour l'authentification des utilisateurs. Les annuaires LDAP offrent une réponse à ce problème en proposant de centraliser les informations par le biais d'un protocole standardisé.
Un serveur LDAP agit en tant qu'intermédiaire entre une base de données et un client.

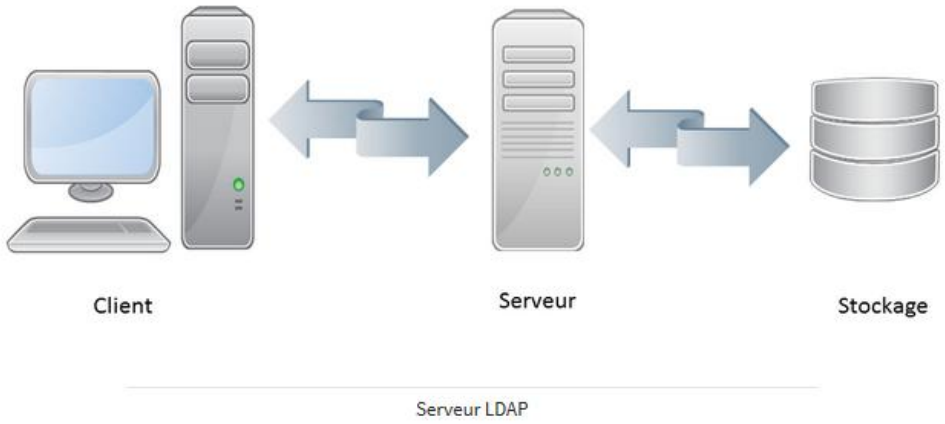


Figure 1: Echange entre un client et un serveur LDAP

Le LDAP représente les informations sous forme d'une arborescence d'informations hiérarchique appelée DIT (Directory Information Tree), dans laquelle les informations, appelées entrées sont représentées sous forme de branches.
Une branche située à la racine d'une ramification est appelée racine.

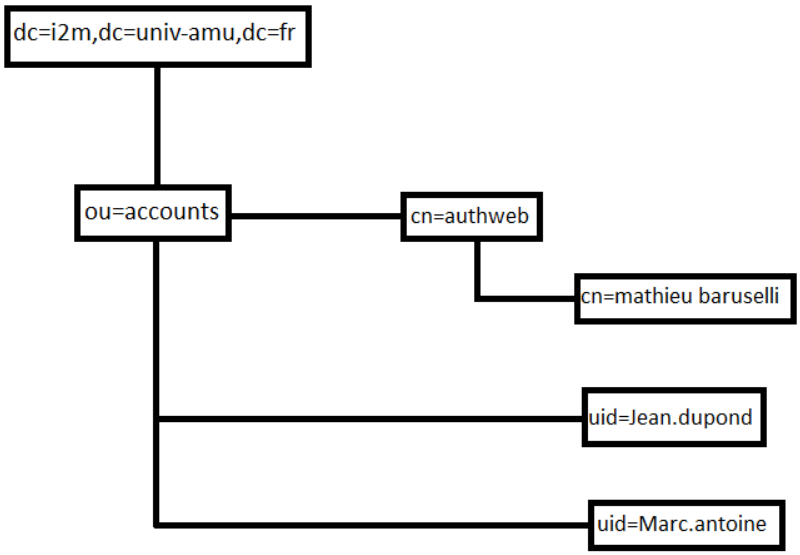


Figure 2: DIT de l'I2M.

b. L'utilisation du LDAP dans l'I2M.

Dans le cas du laboratoire, le LDAP permet d'authentifier un utilisateur sur un machine.
Il est nécessaire, à l'arrivée ou au départ d'une personne de l'ajouter ou bien de la retirer de l'annuaire afin que cette personne puisse utiliser le réseau du laboratoire en fonction de son statut.

La création , la modification, et la suppression d'un utilisateur sont des éléments fastidieux à réaliser pour un administrateur sytème du fait de la complexité et de la longeur de la commande à taper.
L'objectif de cette partie du stage est donc de développer une interface, pour faciliter les interactions avec OpenLDAP.

c. Installation de OpenLDAP sur un serveur.

OpenLDAP est une implémentation Open Sources du protocole LDAP.
C'est un annuaire informatique qui fonctionne sur le modèle client/serveur.
Voici comment il a été installer à l'I2M, sur un serveur debian 8.8.

On installe les paquets openLDAP sur le serveur :

```
$ sudo apt-get update
$ sudo apt-get install slapd ldap-utils
```

On configure le serveur avec l'adresse d'un DNS, un mot de passe, et un format de base de données pour faire fonctionner l'annuaire.

```
$ sudo dpkg-reconfigure slapd
```

Puis on modifie le fichier de configuration du serveur(/etc/lapd/lapd.conf) pour lui assigner l' adresse IP du serveur.

```
BASE    dc=i2m,dc=univ-amu,dc=fr
URI     ldap://10.193.10.30/

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ldap/ca_certs.pem
TLS_REQCERT     allow
~
~
```

Figure 3: Fichier de configuration LDAP.

Le serveur LDAP est maintenant fonctionel, mais n'est pas sécurisé lors d'une demande de connexion.

d. Implémentation d'un annuaire sécurisé.

Le fonctionnement du LDAP repose sur la norme TCP/IP et le port 389 d'un serveur.
Afin de rendre la connexion d'un client au serveur LDAP sécurisée il est nécessaire d'implementer sur le serveur un mécanisme de certificat d'authentification.
Le mécanisme sécurisé utilisé pour communiquer de cette façon se nomme "StartTLS".
Il établit une connexion sécurisée entre le client et le serveur en utilisant la technique TLS(Transport LayerSecurity).

Cette sécurisation opère sur deux points :

-la confidentialité des données.

-l'intégrité des données.

Voici un représentation schématique d'un échange de connexion entre un client et un serveur LDAP:

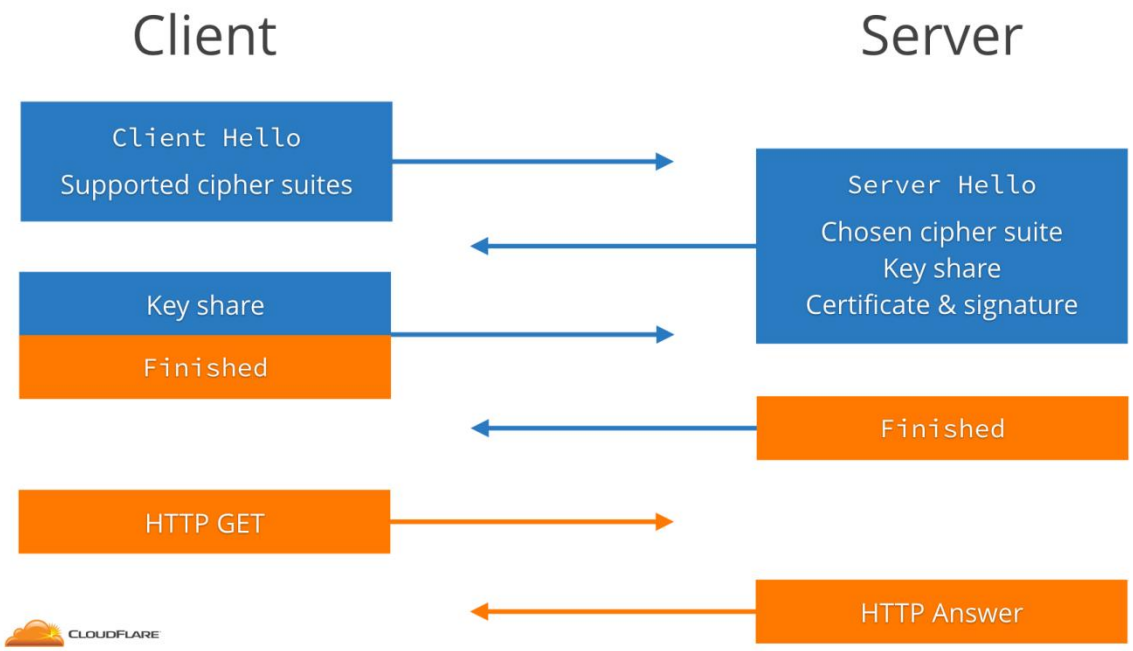


Figure 4: Echange TLS entre un client et un serveur.

Pendant la négociation TLS, le serveur envoie son certificat au client pour prouver son identité.
Le certificat est créé par le serveur préalablement et sa position est indiquée dans le fichier de configuration du serveur.

3. Simplification de la gestion de l'annuaire.

a. Cahier des charges de l'interface LDAP.

Une fois OpenLDAP installé et configuré de manière sécurisée, il convient de commencer la mise en place d'un interface web de gestion de celui-ci.
Dans notre cas la liste des utilisateurs présents dans l'annuaire ont été importés depuis un ancien serveur LDAP.

L'interface web de gestion du LDAP doit permettre de réaliser le plus facilement possible des requêtes sur l'annuaire informatique.
Pour cela, il est donc nécessaire de mettre en place un serveur web afin de pouvoir héberger un site.
Dans notre cas, il s'agit d'un serveur web nommé Apache2, configuré pour recevoir des requêtes sécurisé HTTPS.
Afin de créer une interface "User-Friendly" la conception du service nécessite plusieurs langages de programmation, pour rendre la tâche la plus agréable à l'utilisateur.

L'application est uniquement destinée au service informatique, une accréditation par Login/Password est donc demandée pour accéder au service.
Pour garantir l'intégrité de l'annuaire, le principe exploité est de rendre les interations entre la page web et le serveur LDAP uniquement accessible à un groupe spécifique.
Ce groupe peut être modifié par un administrateur système en se connectant sur le serveur LDAP.

L'application échange donc de manière sécurisé avec l'utilisateur grâce au protocole HTTPS.
La sécurité de la connexion au serveur est garantie par le certificat TLS et l'exécution des scripts d'interaction client serveur est réservé des membres spécifiques.

L'application propose plusieurs fonctionnalitées:

-L'ajout d'un utilisateur au LDAP de l'I2M.
-La suppression d'un utilisateur au LDAP de l'I2M.
-La modification d'un utilisateur au LDAP de l'I2M.
-L'ajout d'un utilisateur au LDAP de l'I2M depuis le LDAP d'AMU.

De plus, l'intégralité des actions effectuées sur le serveur doivent être enregistré, pour retracer l'historique des modifications de l'annuaire en cas de problème.

b. Détails de conception du site web.

Une application web comprend deux grandes parties, le côté client pour la saisie de données de la part des utilisateurs, et le côté serveur pour les interactions avec l'annuaire LDAP.
Pour proposer une interface web moderne du côté client, le moyen le plus adapté pour notre application est de concevoir un site a l'aide du framework Bootstrap.

Bootstrap est une collection d'outils utile à la création du design de site.
C'est un ensemble qui contient des codes HTML et CSS ainsi que des formulaires, des boutons, et autres outils de navigation interactifs.
Le point fort de cet outil est de rendre rapidement une application web fonctionnelle et responsive Design.

Site Web sans Bootstrap:

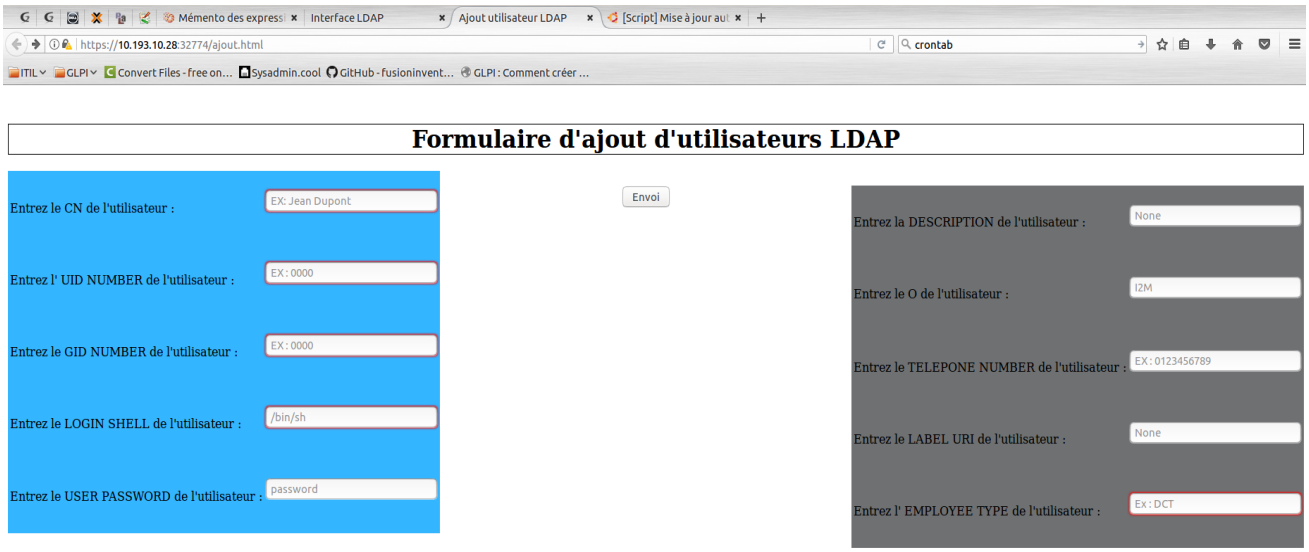


Figure 5: Application sans Bootstrap.

Site Web Avec Bootstrap:

Figure 6: Application avec Bootstrap.

c. Création des fonctionnalités de navigation avancé.

Par ailleurs, pour rendre le site dynamique et donc agréable à l'utilisation, l'implémentation des solutions AJAX et jQuery sont très puissantes.
Ces bibliothèques peuvent comme dans notre cas, permettre la création d'une auto-complétion (Complètement automatique de la saisie au clavier).

jQuery est une bibliothèque JavaScript libre créée pour faciliter l'écriture de script coté client dans le code des pages web.
Ajax, quant-à-lui, permet de construire des sites web dynamiques et interactifs du côté client afin d'améliorer la maniabilité et le confort d'utilisation de celui-ci.

Le confort d'utilisation proposé par cette solution permet à un utilisateur de gagner du temps et rendre l'utilisation quotidienne du site simple.
Voici un exemple de l'auto-complétion mise en place sur l'application grâce à ces solutions :

Figure 7: Présentation de l'auto-complétion.

d. Principe des interactions avec l'annuaire.

Les échanges entre l'annuaire LDAP et l'interface sont réalisés par la partie serveur de l'application.
Le PHP et les fonctions qui lui sont associées permettent d'interroger et de modifier l'annuaire OpenLDAP.
Le point fort du PHP est d'être un langage de programmation libre extrêmement documenté, principalement utilisé pour produire des pages web dynamiques.
Il permet, en autre, de récupérer les données saisies du côté client pour les envoyer au serveur LDAP.
Pour l'application qui a été créée a l'I2M le PHP fonctionne en quatre grandes étapes :

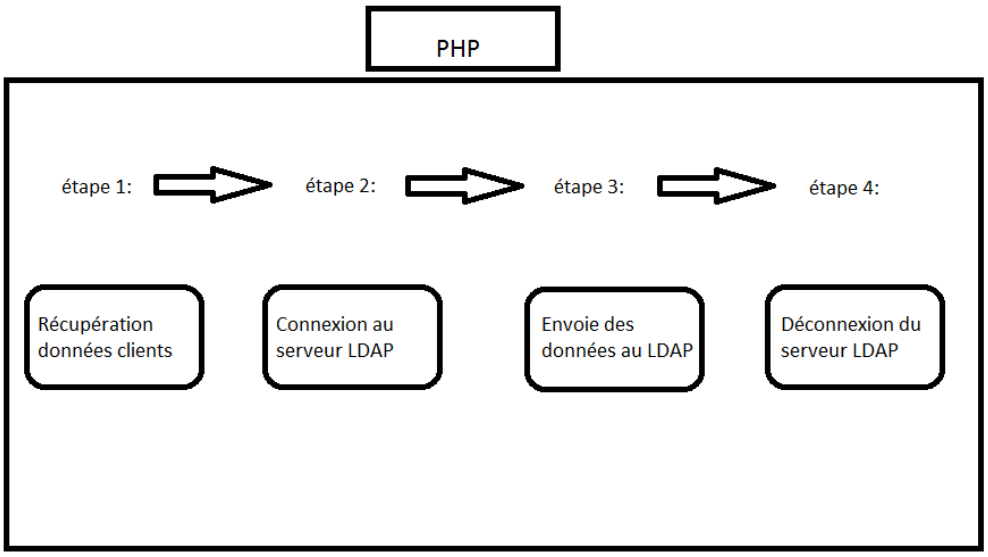


Figure 8: Schéma de fonctionnement de l'application.

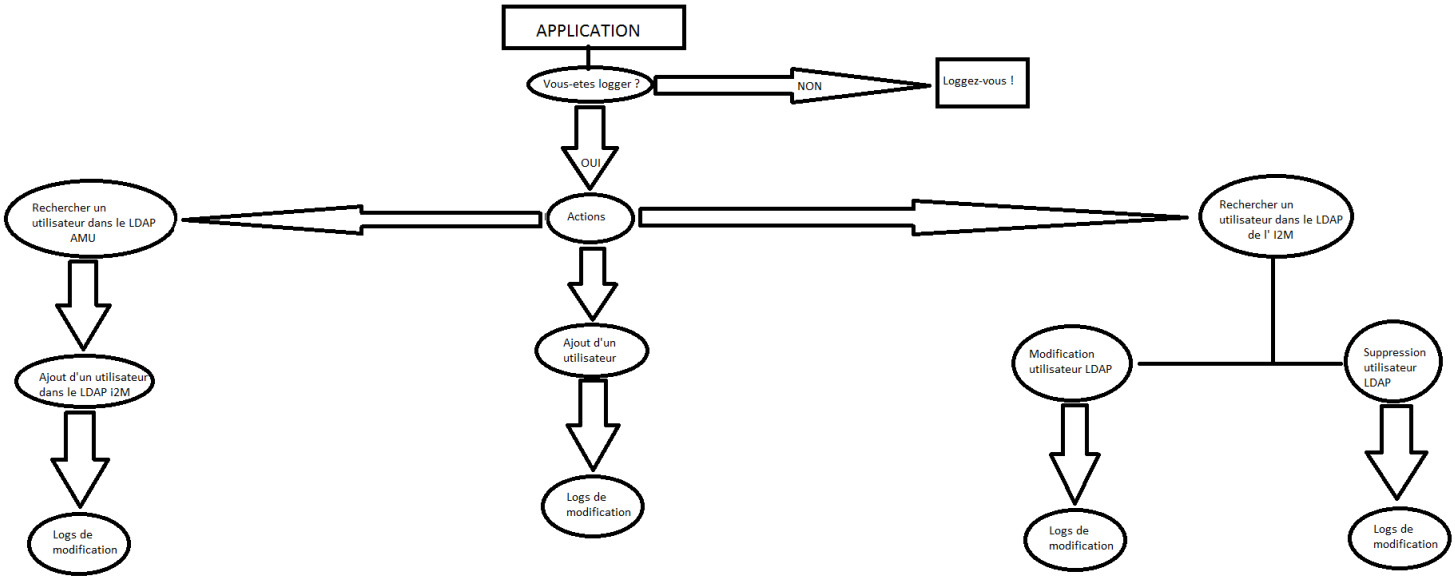
L'intégralité de ces étapes sont controlées pas des scripts PHP.

e. Détails du fonctionnement de l'application.

Le principe de fonctionnement simplifié de l'application peut être comparé à un arbre de décisions. Chaque modification dans l'annuaire nécessite des droits d'authentification spécifiques donnés par le LDAP.

Les accréditations sont gérées par un script PHP, qui à chaques actions vérifie l'identité par l'intermédiaire de sessions.
Les sessions sont un moyen simple de stocker des données individuelles pour chaque utilisateur en utilisant un identifiant de session unique, si la session n'est pas valide la page web affiche un message d'erreur.

Figure 9: Schéma détaillé du fonctionnement de l'application.



f. Sauvegarde des modifications de l'annuaire.

Afin de pouvoir surveiller les modifications apportées au LDAP, l'intégralité des opérations sur l'annuaire sont écrites automatiquement dans un fichier texte.
Ce fichier texte comprend le nom, le prénom et l'adresse IP de la personne aillant fait la modification, ainsi que l'heure et la date du changement.
De plus, le fichier précise aussi l'identité de l'individu créé dans l'annuaire.

Le fichier des logs est conçu pour s'archiver et se supprimer automatiquement au bout d' une semaine afin de garder une trace des opérations.
En cas d'attaque informatique sur l'application, il est donc avantageant d'avoir un système de log comme celui-ci.

Les logs sont basés sur les sessions PHP servant à identifier un utilisateur.

Figure 10: Apercu du fichier des logs.

```
ldap@ldap: ~

147.94.65.153:mathieu baruselli a ajouté un utilisateur Test Test au LDAP le: jeudi 01 juin 2017 à:  14:44
147.94.64.227:mathieu baruselli a ajouté un utilisateur Test Test au LDAP le: jeudi 01 juin 2017 à:  14:45
147.94.64.227:mathieu baruselli a supprimé l'utilisateur test.test du LDAP le: jeudi 01 juin 2017 à:  14:45
147.94.65.153:mathieu baruselli a ajouté un utilisateur Olivier Robert au LDAP le: mardi 06 juin 2017 à:  09:17
147.94.65.153:mathieu baruselli a modifié l'utilisateur olivier.robert du LDAP le: mardi 06 juin 2017 à:  09:29
147.94.65.153:mathieu baruselli a modifié l'utilisateur olivier.robert du LDAP le: mardi 06 juin 2017 à:  09:34
147.94.65.153:mathieu baruselli a modifié l'utilisateur olivier.robert du LDAP le: mardi 06 juin 2017 à:  09:39
~
~
~
~
```

4. Conception de l'application d'annuaire.

a. Les fonctions de connexions PHP pour le LDAP.

La bibliothèque fournie avec PHP donne accès à l'intégralité des fonctions nécessaire pour communiquer avec un annuaire OpenLDAP.
Lorsqu'un utilisateur effectue une requête sur l'application automatiquement un script PHP exécute les actions demandées.
Nous allons voir comment les scripts PHP se connectent à l'annuaire.

Pour se connecter à un serveur LDAP via un script PHP, plusieurs données sont demandées :

-L'adresse IP du serveur.
-La racine de l'utilisateur root.
- le mot de passe root.

```php
<?php

    //Paramètres de connexion au serveur.
    $ldap="10.193.10.30";
    $usr="cn=admin,dc=i2m,dc=univ-amu,dc=fr";
    $pwd="FalsePASSWORD";
```

Figure 11: Paramètres de connexion serveur LDAP pour PHP

Les fonctions de connexion et d'initialisation de requêtes au LDAP se nomment respectivement "ldap_connect" et "ldap_bind" elle permettent d'initialiser la connexion avec le serveur.
Notre annuaire étant sécurisé, il est donc nécessaire de le préciser lorsque l'on souhaite établir une connexion avec le serveur.
Pour cela il faut donc annoncer l'utilisation de la couche TLS.

```php
$ds=ldap_connect($ldap);
    if ($ds) {
       ldap_set_option($ds, LDAP_OPT_PROTOCOL_VERSION, 3);
       ldap_start_tls($ds);
       $ldapbind = ldap_bind($ds,$usr,$pwd);
    }
    return $ds;
```

Figure 12: Options de connexion au serveur LDAP

Une fois la connexion établie et l'authentification réalisée grâce au paramètres précédents, le serveur retourne un numéro d'identification unique qui permet d'exécuter des modifications sur l'annuaire.
Cette valeur sera utilisée par toutes les fonctions de modifications PHP.

b. Les sessions, une authentification sure !

Pour avoir accès aux modifications du LDAP un utilisateur doit appartenir à une branche spécifique de l'annuaire spécifique nommé authWeb.
Les champs login et password permettent de vérifier l'identité d'une personne ainsi que son appartenance au groupe authWeb .
Sans cela, l'utilisateur ne peut effectuer aucune requête.

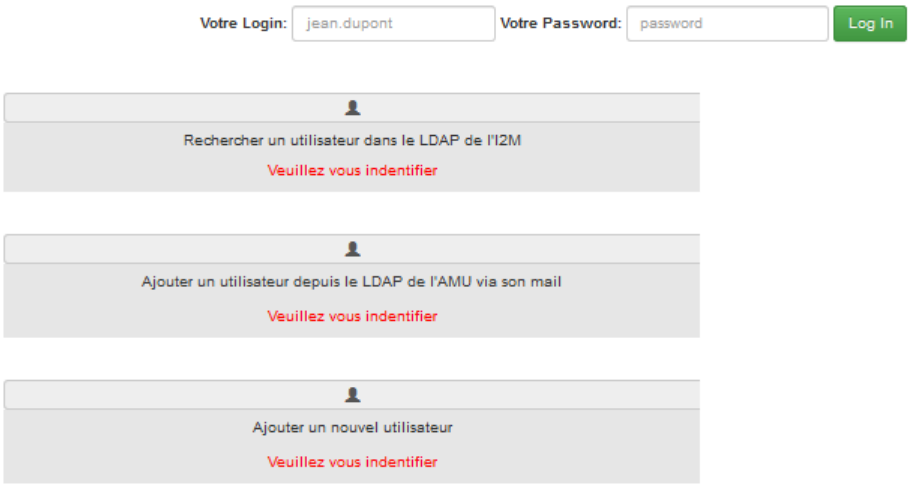


Figure 13: Page de login de l'application.

Afin de vérifier les données saisies par l'utilisateur et de lui permettre de naviguer sur les pages du site, un script PHP s'exécute.
Si les données sont correctes, l'utilisateur obtient un droit d'entre par le biais d'une session.
Sans une session valide l'utilisateur ne peut pas modifier l'annuaire.

```php
$login=$_POST['login'];
$mdp=$_POST['mdp'];

$dn = "cn=$login, cn=authweb, ou=accounts, dc=i2m, dc=univ-amu, dc=fr";
$attr = "cn";
    $value = $login;
$attrp = "userPassword";
    $encrypt = '{MD5}' . base64_encode(pack('H*',md5($mdp)));
    $valuep = $encrypt;

$r=ldap_compare($ds, $dn, $attr, $value);
$s=ldap_compare($ds, $dn, $attrp, $valuep);


    if ($r === true && $s === true)  {
     echo '<script type="text/javascript">alert("Authentification correcte");</script>';
     echo "<script type='text/javascript'>document.location.replace('index.php');</script>";
         session_start ();
     $_SESSION['login'] = $_POST['login'];
 } else {
    echo '<script type="text/javascript">alert("Erreur d\'acc\350s");</script>';
    echo "<script type='text/javascript'>document.location.replace('weblog.php');</script>";
    }

} else {
echo "Connection LDAP error !";
}
```

Figure 13: Script PHP de login

Il faut noter que le mot de passe subit un hachage dans le ldap et n'est donc pas stocké en clair dans l'annuaire.

c. Modifier, ajouter, supprimer un utilisateur.

L'intégralité des modification que l'on souhaite faire sur le LDAP par l'utilisation du PHP, nécessite le paramètre de connexion au serveur récupéré précédement.

Grâce à ce paramètre et aux fonctions PHP nommées ldap_delete, ldap_add et ldap_modify il est possible de supprimer, modifier ou ajouter un utilisateur.
En outre, ces fonctions nécessites des informations relative à l'usage pour pouvoir fonctionner convenablement.
Il sera donc nécessaire d'indiquer le nom de la personne à supprimer pour la retirer de l'annuaire.

L'intégralité de ces information sont définit par le protocole LDAP par un schéma strict.
Voici la correspondance entre le tableau PHP et le schéma du LDAP :

```php
$uidn=$_POST['uidn'];
if (empty($uidn)) {
    echo " ";
} else {
    $info['uidnumber']=$uidn;
}

$gidn=$_POST['gidn'];
if (empty($gidn)) {
    echo " ";
} else {
    $info['gidnumber']=$gidn;
}

$gecos=$_POST['gecos'];
if (empty($gecos)) {
    echo " ";
} else {
    $info['gecos']=$gecos;
}

$shell=$_POST['shell'];
if (empty($shell)) {
    echo " ";
} else {
    $info['loginshell']=$shell;
}

$home=$_POST['home'];
if (empty($home)) {
    echo " ";
} else {
    $info['homedirectory']=$home;
}
```

Figure 13: Script PHP de modification d'annuaire.

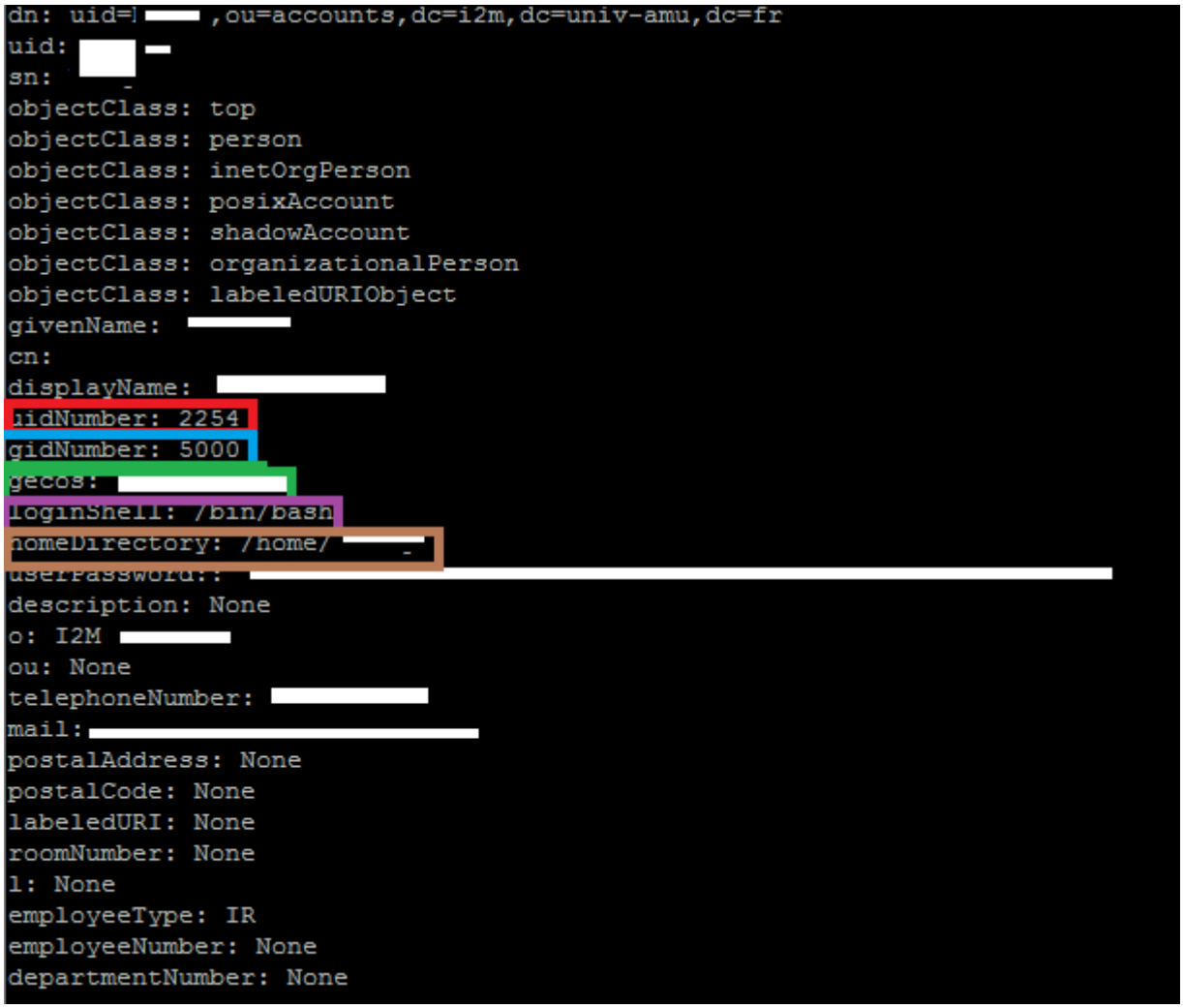


Figure 14: Schéma du annuaire LDAP.

On observe que les valeurs renseignées dans le tableau PHP correspondent au schéma du LDAP définit par la norme X500.
Si une des informations nécessaires à l'exécution d'une fonction est manquante, la modifications ne sera pas effectuée.
La correspondance présente ci dessus par le code couleur reflète le schéma.

5. Amélioration de la sécurité des équipements réseaux.

a. Modèles réseaux.

Le parc informatique de l'I2M, et plus précisément sur le site de Château-Gombert, est composé d'équipements réseaux de modèle HP 2610et 2626 ainsi que des CISCO 2948 G.
Historiquement, les postes de travail des utilisateurs étaient des Sun Microsystem, ils fonctionnaient donc à l'aide d'un serveur interne Sun.
De nombreux vlans était encore configurés sur les switchs.

L'objectif qu'il m'a été attribué était de supprimer les vlans inutilisés et d'améliorer la sécurité de ces équipements réseau.

b. Modifications des configurations réseaux.

Afin de garantir un maximum de sécurité sur les équipements réseaux, plusieurs modifications ont été apportées aux switchs.

D'abord, la mise en place d'une bannière de prévention afin de se prémunir sur le plan légal à l'encontre d' un potentiel attaquant.

```
banner motd "This is a private system maintened by the Institut of Mathemetics o
f Marseille. Unautorized use of this system can result in civil and criminal pen
alities ! "
```

Figure 15: Bannière d'un switch HP.

Par ailleurs, la méthode de connexions à distance des commutateurs a évolué du protocole telnet où les mots de passe sont transmis en clair, pour le protocole SSH ou les informations de connexions sont chiffrées. Le port de connexions par défaut du ssh a été changé.

```
Switch(config)# ip ssh

Switch(config)# ip ssh port 2262

Switch(config)# ip ssh key-size 2048

Switch(config)# crypto key generate ssh rsa

Switch(config)# ip ssh timeout 300

Switch(config)# no telnet-server
```

Figure 16: Fichier de configuration SSH d'un commutateur HP.

De même, la connexion par page web aux équipements utilise le protocole HTTP où la aussi les informations ne sont pas chiffrées. Pour parfaire la sécurité, le protocole HTTPS a été mis en place.

```
Switch(config)# crypto key generate cert 2048

Switch(config)#  crypto host-cert generate self-signed
01/01/2050 HostnameSwitch I2M autoI2M

Switch(config)# web-management ssl

Switch(config)# no web-management plaintext
```

Figure 17: Fichier de configuration HTTPD d'un switch HP.

De plus, tous les vlans inutilisés ont été supprimés, leurs nombre est passé de 7 à 3:

Voici l'ancienne configuration des vlans:

```
vlan 1
   name "DEFAULT_VLAN"
   untagged 25-26
   ip address dhcp-bootp
   no untagged 1-24
   exit
vlan 200
   name "TOIP2"
   tagged 1-26
   voice
   exit
vlan 21
   name "CMI-rech"
   untagged 2-24
   ip address 147.94.65.59 255.255.254.0
   tagged 25-26
   exit
vlan 22
   name "CMI-ens"
   tagged 25-26
   exit
vlan 24
   name "CMI-sunray"
   tagged 25-26
   exit
vlan 27
   name "jumpstart-re"
   tagged 25-26
   exit
vlan 114
   name "PedagoPriv"
   untagged 1
   tagged 25-26
   exit
```

Figure 18: Vlans d'un équipement réseau HP

Voici la configuration actuelle des vlans:

```
vlan 1
   name "DEFAULT_VLAN"
   untagged 25-26
   ip address dhcp-bootp
   no untagged 1-24
   exit
vlan 200
   name "TOIP2"
   tagged 1-26
   voice
   exit
vlan 21
   name "CMI-rech"
   untagged 2-24
   ip address 147.94.65.59 255.255.254.0
   tagged 25-26
   exit
```

Figure 19: Vlans modifiés d'un switch HP.

c. Analyse des failles réseau.

Après avoir appliqué des changements sur les équipements réseaux, il est nécessaire d'observer le résultat de ces modifications sur la sécurité du laboratoire, ainsi que de corriger d'éventuelles failles de sécurité.
Les failles de sécurité présentes dans un réseaux d'entreprise peuvent compromettre l'intégralité des services, il est donc primordiale pour un organisme d'avoir un oeil attentif sur le sujet.

Nessus est un scanner de sécurité réseaux, capable d'analyser l'intégralité d'une plage réseau pour détecter des potentiels vecteurs d'attaques de tous types.

Ce logiciel est destiné aux entreprises du fait de sa licence payante, mais il existe un version gratuite nommé Nessus Home, qui est utilisable sur un nombre limité de machines.

Pour Initialiser un scan avec cet utilitaire il suffit de se connecter sur son interface web apres l'avoir installée.
La prise en main du scanner est intuivite et rapide, voici l'interface de configuration d'un scan Nessus:

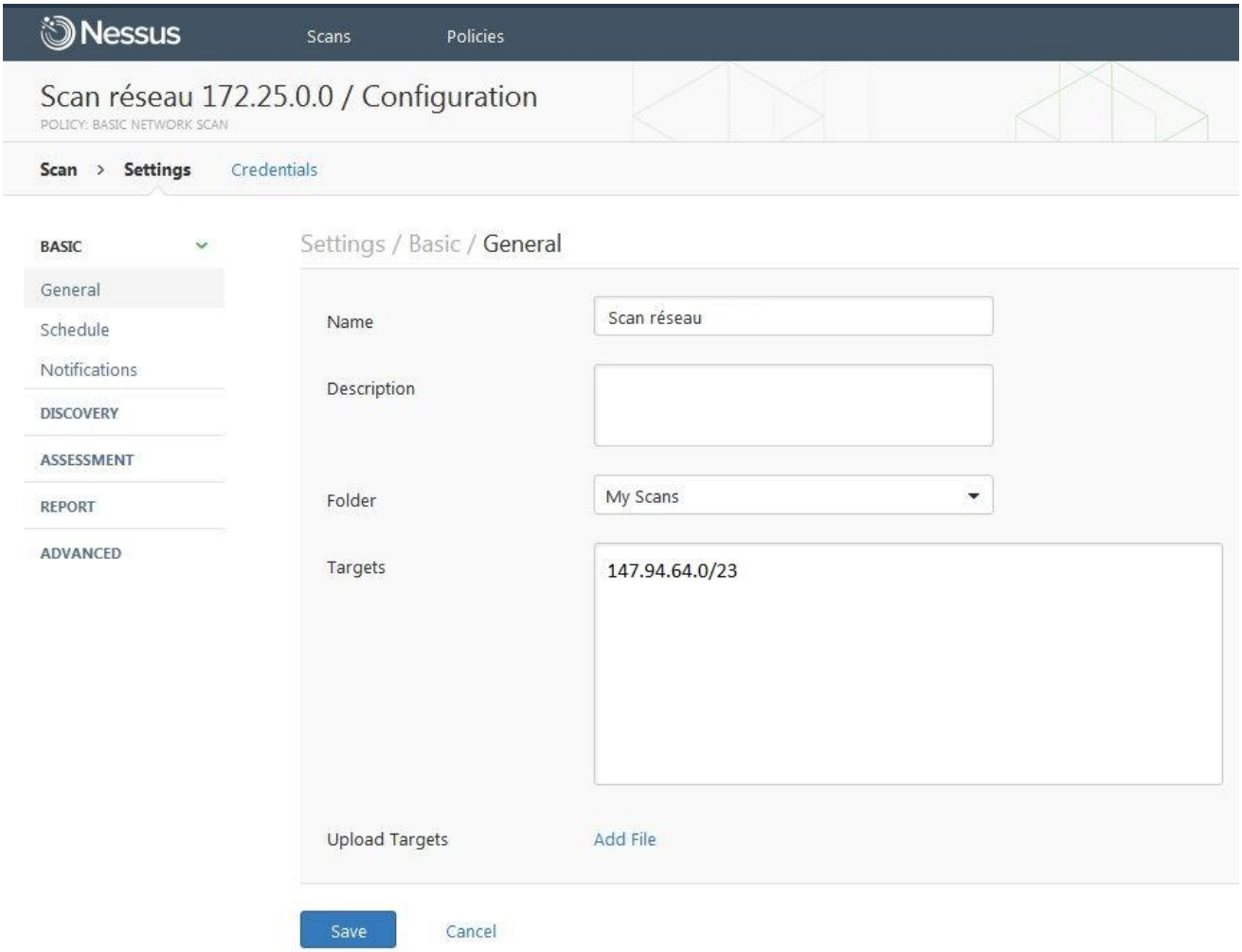


Figure 20: Page web de paramétrage Nessus.

Une fois le scan des machines terminé, l'application web nous retourne pour chaques machines présente sur le réseaux un descriptif des vulnérabilités, ainsi qu'un récapitulatif globale.

Details

Severity	Plugin Id	Name
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access
High (7.5)	42424	CGI Generic SQL Injection (blind)
Medium (6.8)	90509	Samba Badlock Vulnerability
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
Medium (4.3)	62565	Transport Layer Security (TLS) Protocol CRIME Vulnerability
Medium (4.3)	85582	Web Application Potentially Vulnerable to Clickjacking
Medium (4.3)	90317	SSH Weak Algorithms Supported
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm

Figure 21: Récapitulatif des vulnérabilités d'une machine après un scan.

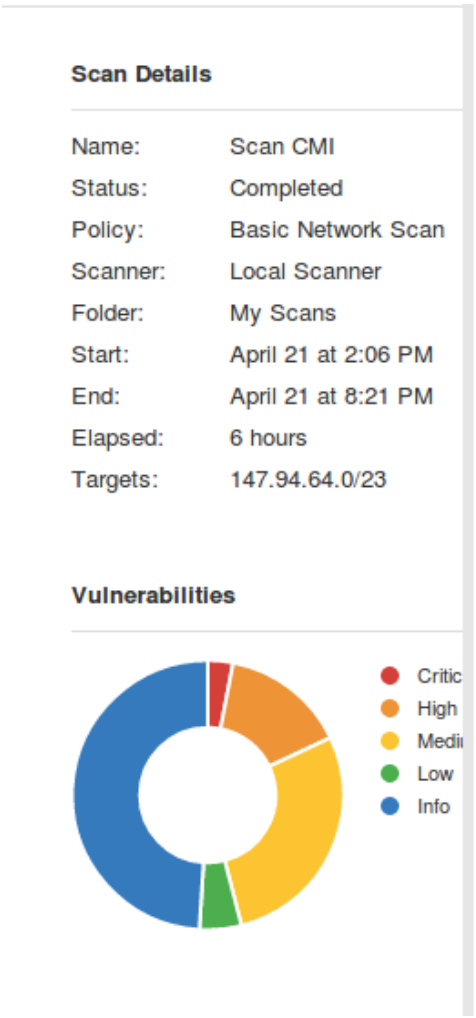


Figure 22: Récapitulatif des vulnérabilitées générale après un scan.

Grâce à un base de données propre au programme qui contient différents type de vulnérabilités, Nessus peut détecter les failles de sécurité présentes sur des machines ou des serveurs.
De plus, il est capable de tester des mots de passe par défaut sur certain service et peut même être couplé avec le paquet Hydra pour effectuer des attaques par dictionnaires.

Nessus se sert de sa base de connaissance pour répertorier le niveau de gravité de faille.
Le seuil varie entre 0 et 10. Ce dernier étant un faille critique.

L'objectif est donc de comparer les vulnérabilités observées sur les équipements réseaux la présence de brèches dans le parc informatique avant et après les modifications des configurations.
Avant l'application de la modification des configurations, on observe que le serveur Telnet est bien présent sur le commutateur.

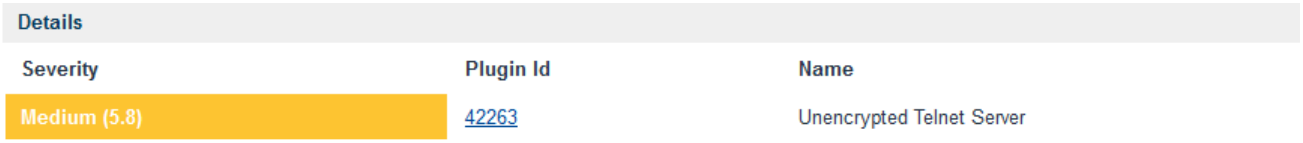


Figure 23: Vulnérabilité Telnet

Après l'application de la modification des configurations le serveur Telnet n'est plus une vulnérabilité, il a été retiré de la liste..
De même le HTPP n'est plus présent, car le HTPPS a été configurer.

Figure 24: Application de modifications HTTPS.

d. Corrections de mots de passe par défaut.

Le parc informatique de l'institut est composé de serveurs Dell pour de nombreux services et applications d'entreprise.
Ces serveurs Dell ont la particularité de disposer d'un controleur nommé IDRAC qui permet a un utilisateur de se connecter avec un login et un mot de passe sur le serveur.
IDRAC permet d'obtenir un visuel à distance de l'état d'un serveur et d'avoir accès a son terminal.
Cela reviendrait à se trouver dans la salle des serveurs.
Avec cette technologie il est donc possible d'allumer ou d'éteindre un serveur à distance, et de l'administer.

La connexion à l'IDRAC s'effectue par un page web, Nessus teste donc de se connecter sur l'application web du contrôleur avec les mots de passe par défaut du constructeur systématiquement.

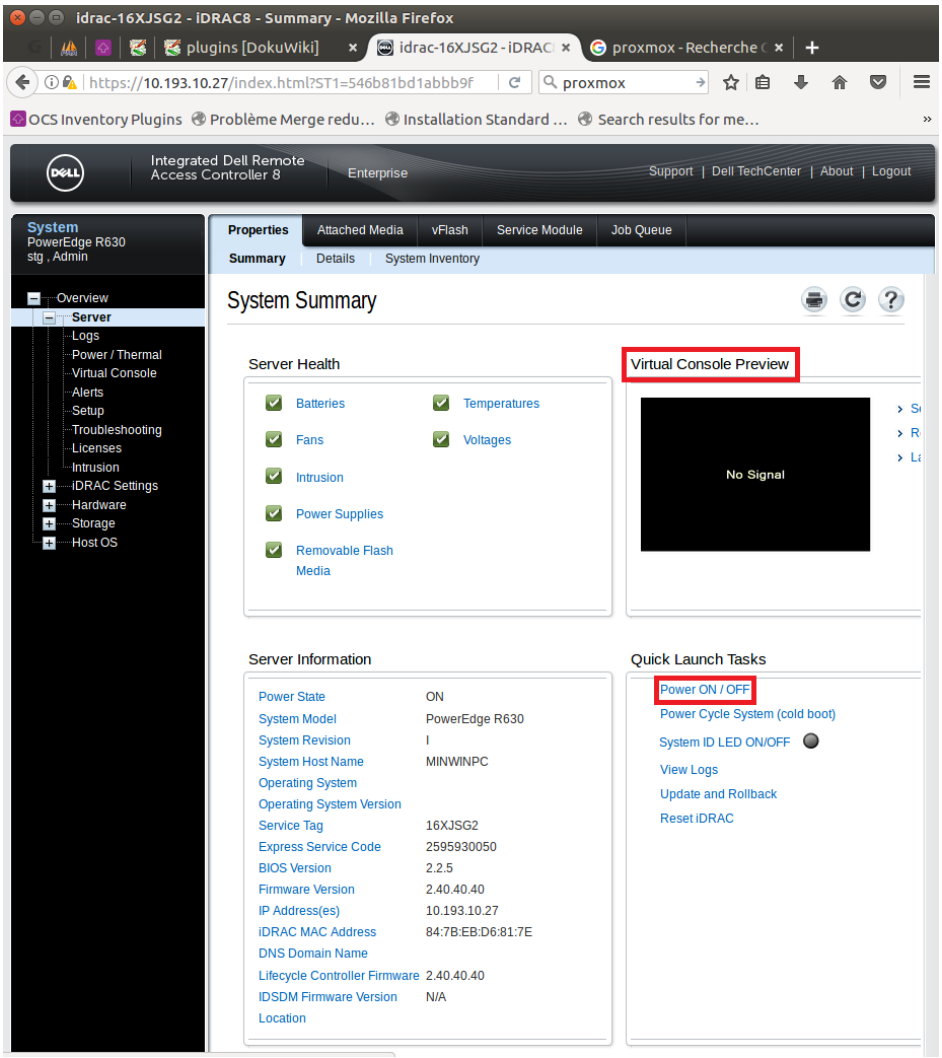
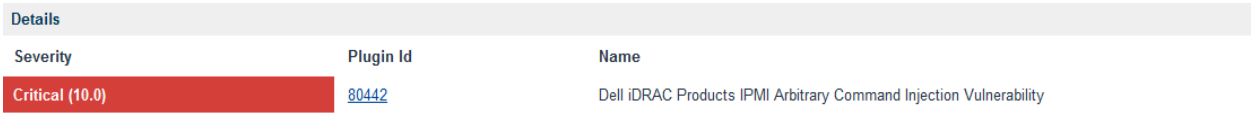


Figure 25: Controlleur Dell IDRAC.

Dans notre cas, celui-ci a réussi, ce qui constitue une faille critique de niveau 10, qui se retrouve sur 4 des 5 serveurs de l'entreprise.

Figure 26: Présence d'un faille critique sur un serveur.



Même si les serveurs ne sont accessibles depuis l'extérieur, cela représente un danger potentiel qui a été corrigé.
Nessus a permis de corriger d'autres failles dans le laboratoire, comme par exemple la détection de mot de passe faible sur un NAS des chercheurs du laboratoire.

II. III.Conclusion.

III. IV.Glossaire.

DOSI: Direction Opérationnelle des Sytèmes d'information, a pour mission de mettre en oeuvre la politique de l'université d'Aix-Marseille en matière de systémes informatiques.
CNRS: Centre National de Recherche Scientifique, est un organisme public de recherche.
I2M: Institut de Mathématiques de Marseille.
NAT: Network Address Translation, il s'agit d'un mécanisme de traduction d'adresses permet a plusieurs individus de naviguer sur internet avec une seul adresse public.
Unix: Il s'agit d'un système d'exploitation multi-tâche.
Virtualisation: Permet de simuler l'existence du matériel et de créér un système informatique virtuel.
Proxmox: Il s'agit d'une solution de virtualisation libre.
Bash: Bourne-Again Shell, est un interpréteur de commandes sous Linux.
Hyperviseur: Cela correspond à une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler simultanement.
KVM: Kernel-based Virtual Machine, est un hyperviseur libre pour linux.
Debian: Il s'agit d'un sytème d'exploitation et d'une distribution de logiciels libre.
RAID: Il s'agit d'un ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer la sécurité et la tolérance aux pannes.
Supervison Réseau: C'est un ensemble de technique permettant de contrôler l'état d'un réseau d'une entreprise en temps direct.
Shinken/IcingaII: Deux solutions libres de supervison.
Open Source: Cela correspond à la libre distribution et modification d'un code informatique.
LDAP: Lightweight Directory Access Protocol est à l'origine un protocole d'interrogation et de modification d'annuaire.
OpenLdap: Il s'agit d'une implémentation libre du protocole LDAP.
DIT: Directory Inormation Tree, correspond à une arborescence informatique d'un annuaire.
TCP/IP: Cette suite de protocoles est utilisés pour le transfert de données sur internet.
TLS: Transport Layer Security, est un protocole d'authentification client-serveur.
NAS: Network Attached Stroage, est un serveur de stockage en réseau.
Wiki: Il s'agit d'une application web qui permet la création de documentation informatique.
PHP: Il s'agit d'un language de programmation libre souvent utilisé pour le développement web.
Boostrap: Il s'agit d'un ensemble d'outils de création de design pour les sites web.
HTML: HyperText Markup Language est un format de données conçu pour les pages web.
CSS: Il s'agit d'un language qui décrit l'apparence d'une page web.
Responsive Design: Il s'agit d'une solution qui consiste à rendre un site web adaptatif en fonction d'un écran.
jQUERY: Il s'agit d'une fonctionnalité qui permet de rendre un site web dynamique.
AJAX: Permet de modifier le contenu d'un page web sans la recharger.
Logs: Historique des actions effectuer sur un service.
Vlan: Il s'agit d'un réseaux informatique indépendant.
Telnet: Terminal Network, est un protocole de connexion à distance non sécurisé.
SSH: Secure Shell, est un protocole de connexion à distance sécurisé.
HTTP: Hypertext Transfer Protocol, est un protocole de communication client-serveur.
HTTPS: Hypertext Transfer Protocol Secure, est un protocole de communication client-serveur qui utilise une couche de sécurité TLS.
Hachage: Il s'agit d'un fonction permettant de rendre illisible une chaîne de caractères.
DNS: Domain Name System, est un service permettant de traduire un nom de domaine en adresse IP.
Framework: Il s'agit d'un ensemble de composant logiciels structurels servant a créer les fondations d'une partie d'un logiciel.

IV. V.Bibliographie.

Documentation technique sur l'interface web du LDAP :

http://php.net/manual/fr/book.ldap.php
http://getbootstrap.com/
https://jquery.com/
https://openclassrooms.com/courses/apprenez-a-creer-votre-site-web-avec-html5-et-css3/mise-en-page-adaptative-avec-les-media-queries
https://www.devbridge.com/sourcery/components/jquery-autocomplete/
http://api.jquery.com/jquery.ajax/

Documentation technique sur les équipements réseaux :

https://supportforums.cisco.com/document/12991286/cisco-catos-vs-ios-commands
http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c02564134
http://whp-hou9.cold.extweb.hp.com/pub/networking/software/2600-Install-Mar06-59912165.pdf

Docuentation sur la mise en place d'un LDAP sécurisé :

https://www.digitalocean.com/community/tutorials/how-to-encrypt-openldap-connections-using-starttls
https://www.digitalocean.com/community/tutorials/how-to-create-a-ssl-certificate-on-apache-for-ubuntu-14-04

Documentation sur l'implentation d'un serveur de virtualisation Proxmox :

https://www.proxmox.com/en/
https://pve.proxmox.com/wiki/Network_Model

Documentation sur l'analyseur de vulnérabilité Nessus :

https://mondedie.fr/d/5860-Tuto-Auditer-son-systeme-avec-Nessus

Documentation technique sur la technologie RAID :

http://www.supinfo.com/articles/single/1176-raid-ses-differents-types

VI.Annexes.

Journal de bord:

Conception de l'interface de l'annuaire:

Conception de l'interface d'automatisation du dhcp: